uFR Desfire® example C console

Version 1.3.

Table of contents

1. Application overview

Link: https://git.d-logic.net/nfc-rfid-reader-sdk/ufr-ds-examples-c.git

When you start application, it looks like this:

```
Select reader opening mode:
(1) - Simple Reader Open
(2) - Advanced Reader Open
1
-----------------------------------------------------------
        uFR NFC reader successfully opened.
        Firmware version 255.100.26
-----------------------------------------------------------
        AES key: 00000000000000000000000000000000
        AID 3 bytes hex: A10000
        AID key number for auth: 0
        File ID: 3
        Internal key number: 125
-----------------------------------------------------------
+---------------------------------------------------------+
:                  uFR Desfire example                    :
:                      version 1.3                        :
+---------------------------------------------------------+
                                    For exit, hit escape.
-----------------------------------------------------------
(0) - Change authentication mode
(1) - Master key authentication
(2) - Get card UID
(3) - Format card
(4) - DES to AES
(5) - AES to DES
(6) - Get free memory
(7) - Set random ID
(8) - Internal key lock
(9) - Internal key unlock
(a) - Set baud rate
(b) - Get baud rate
(c) - Store key into reader
(d) - Change key
(e) - Change key settings
(f) - Get key settings
(g) - Make application
(h) - Delete application
(j) - Make file
(k) - Delete file
(l) - Write Std file or record
(m) - Read Std file or records
(n) - Read Value file
(o) - Increase Value file
(p) - Decrease Value file
(q) - Clear Record file
(r) - Get application IDs
(s) - Store key into SAM
(t) - Change config parameters
```

Key for authentication, AID, AID key number for authentication, File ID and internal key index are read out from config.txt file.

1.1. Config file explanation (config.txt)

Configuration file config.txt is loaded when the application starts. There are key for authentication, AID, ordinal number of key in AID for authentication, File ID and internal key index (when key stored into reader).
File structure:
DES key: 0000000000000000
AID 3 bytes hex: 000000
AID key number for auth: 0
File ID: 1
Internal key number: 0
First line contains key type, and hexadecimal value of key.
If key type is DES (8 bytes) then 16 characters must be entered (DES key: 0102030405060708)
If key type is 2K3DES (16 bytes) then 32 characters must be entered (2K3DES key: 01020304050607080910111213141516)
If key type is 3K3DES (24 bytes) then 48 characters must be entered (3K3DES key: 010203040506070809101112131415161718192021222324)
If key type is AES (16 bytes) then 32 characters must be entered (AES key: 01020304050607080910111213141516)
Second line contains AID, 6 characters must be entered (AID 3 bytes hex: 010203)
Third line contains ordinal number in application for authentication (0 to maximal number of application keys - 1)
Fourth line contains index of File ID in application. If the function don't use this parameter, then this value be ignored.
Fifth line contains ordinal number of key for authentication stored into reader.

Configuration file can be changed from application when 't' pressed (Change config parameters).
 First, you will see current config.txt file with options 1 - 5 for changing and esc for back to main menu.

```
Current config:
        DES key: 0000000000000000
        AID: 000000
        AID key number auth: 0
        File ID: 1
        Internal key nr: 0
1 - Change key
2 - Change AID
3 - Change AID key number
4 - Change File ID
5 - Change internal key number
esc - Exit to main menu
```

For key changing press '1'. There are four types of key for authentication.

```
Enter key type
1 - DES (8 bytes)
2 - 2K3DES (16 bytes)
3 - 3K3DES (24 bytes)
4 - AES (16 bytes)
```

For example press '3' for 3K3DES key. Enter 24 bytes in hexadecimal format (48 characters).

```
Input new 3K3DES key (24 bytes):
010203040506070809101112131415161718192021222324
1 - Change key
2 - Change AID
3 - Change AID key number
4 - Change File ID
5 - Change internal key number
esc - Exit to main menu
```

When the changing is over, press ESC button for return in main menu, and then press 't' for modification checking.

```
Current config:
        3K3DES key: 010203040506070809101112131415161718192021222324
        AID: 000000
        AID key number auth: 0
        File ID: 1
        Internal key nr: 0
1 - Change key
2 - Change AID
3 - Change AID key number
4 - Change File ID
5 - Change internal key number
esc - Exit to main menu
```

The type and value of authentication key is changed.

1.2. Change authentication mode (0)

There 3 mode of authentication.
SAM key authentication mode available only for uFR Classic CS with SAM and firmware versions 5.100.x.
For firmware versions 5.100.x using of internal and provided key is restricted to AES key only. DES, 2K3DES and 3K3DES keys are can use with SAM only. AES key may uses in all authentication modes.
With regular firmware versions 5.0.x from 5.0.25 all key types may be use. uFR Classic CS with SAM works with firmware versions 5.0.x too.

```
Select authentication mode:
(1) - Internal key
(2) - Provided key
(3) - SAM key
3
Authentication mode is set to SAM KEY
```

1.3. Master key authentication (1)

For switching between master key authentication, press '1' on keyboard.
It looks like this (here is '1' pressed twice):

```
-----------------------------------------------
Master key authentication is not required
-----------------------------------------------
Master key authentication is now required
-----------------------------------------------
```

Whether authentication is required or not, depends on the master key of the card or application settings.

1.4. Get card UID (2)

For card UID (7 bytes) press '2'. Valid authentication with master or application key is required.

```
-----------------------------------------------
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 167 ms
CARD UID = 04658E42EC3580
-----------------------------------------------
```

1.5. Format card (3)

Pressing number '3' on your keyboard will cause formatting card (deleting all applications and files except AID with number: 000000). Depends on which authentication mode you chose, it will look for AES key into reader (INTERNAL KEY) or in config.txt file (PROVIDED KEY).

```
-----------------------------------------------
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 574 ms
Card is formatted
-----------------------------------------------
```

1.6. DES to AES (4)

Changing the card master key from factory DES key 0x0000000000000000 to AES key 0x00000000000000000000000000000000.

1.7. AES to DES (5)

Changing the card master key from AES key 0x00000000000000000000000000000000 to DES key 0x0000000000000000.

1.8. Get free memory (6)

Read the quantity of available memory on the card.

```
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 18 ms
Free memory: 4864 bytes
```

1.9. Set random ID (7)

Activating the random ID card options by Set Random ID button. Required authentication using card master key.

The card returns 4 bytes random ID instead 7 bytes unique ID.

Warning: this operation is irreversible.

When this option is activated, the UID can be read by special command that requires authentication using valid key.

1.10. Internal key lock (8)

You have to enter password (8 characters length) to lock keys enrollment. Factory password is "11111111".

```
Input password (8 characters):
11111111
Operation completed. Status is [0x00 (0)] UFR_OK
```

1.11. Internal key unlock (9)

To unlock the possibility to enroll keys into reader, you must enter the same password to unlock keys which is entered to lock keys enrollment. Factory password is "11111111"

```
Input password (8 characters):
11111111
Operation completed. Status is [0x00 (0)] UFR_OK
```

1.12. Set baud rate (a)

After activating the option 'Set baud rate' by pressing 'a' on keyboard you will see multiple choices to choose for transceive and receive baud rate. Just enter the number next to option you want to choose.

```
-----------------------------------------------------------
Enter value for setting transmit rate (tx speed)
0 - 106 kbps
1 - 212 kbps
2 - 424 kbps
0
Enter value for setting receive rate (rx speed)
0 - 106 kbps
1 - 212 kbps
2 - 424 kbps
0
Operation completed. Status is: [0x00 (0)] UFR_OK
-----------------------------------------------------------
```

1.13. Get baud rate (b)

Read values of transmit and receive baud rate of reader.

```
-----------------------------------------------------------
TX baud rate = 106 kbps;
RX baud rate = 106 kbps;
-----------------------------------------------------------
```

1.14. Store key into reader (c)

First choice the type of key.

```
-----------------------------------------------------------
Enter key type
1 - DES (8 bytes)
2 - 2K3DES (16 bytes)
3 - 3K3DES (24 bytes)
4 - AES (16 bytes)
```

For example choice 3K3DES key. Key 0x0102030405060708091011121314151617181920212223 24.
Internal key index is 0. For 3K3DES keys two key fields into reader will be occupied. In this case 0 and 1.
First free key index is 2. For other key types just one key field will be used.

```
-----------------------------------------------------------
Enter key type
1 - DES (8 bytes)
2 - 2K3DES (16 bytes)
3 - 3K3DES (24 bytes)
4 - AES (16 bytes)
3
Two key fields will be occupied !!!
Enter 3K3DES key (24 bytes):
010203040506070809101112131415161718192021222324
Input reader internal key number (0-15):
0
Operation completed. Status is [0x00 (0)] UFR_OK
-----------------------------------------------------------
```

1.15. Change key (d)

Changing card master, and application master and user keys. When changing master key, then may be change the key type and value of key. Into application all keys are same type, and key type don't be changed.

For example change master key to 3K3DES type, and value
0x010203040506070809101112131415161718192021222324.

```
-----------------------------------------------------
MASTER KEY CHANGE !!!
 Enter new key type
 1 - DES (8 bytes)
 2 - 2K3DES (16 bytes)
 3 - 3K3DES (24 bytes)
 4 - AES (16 bytes)
3
Input new 3K3DES key (24 bytes):
010203040506070809101112131415161718192021222324
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 100 ms
-----------------------------------------------------
```

1.16. Change key setting (e)

For changing key settings, carefully read available settings and chose one. Take care about setting you chose, some of them cannot be changeable anymore. If you are changing settings for AID 000000 - IT CAN'T BE FORMATTED.

```
-----------------------------------------------------
Choose key settings:
0 - No settings
1 - Settings not changeable anymore
2 - Create or delete application with master key authentication
3 - Master key not changeable anymore
4 - Settings not changeable anymore and create or delete application with master key
5 - Settings and master key not changeable anymore
6 - Create and delete application with master key and master key is not changeable anymore
7 - Settings not changeable anymore, create or delete application with master key, master key is not changeable anymore
```

1.17. Get key setting (f)

Read card master or application master key settings and maximal number of application keys. For example read card master key settings.

```
-----------------------------------------------------
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 160 ms
Maximal number of keys into application: 1
2 - Create or delete application with master key authentication
-----------------------------------------------------
```

1.18. Make application (g)

For example make application with AES keys. AID = 0xA10000. Maximal key number 3.

```
-------------------------------------------------------
Choose application key type:
1 - DES
2 - 3K3DES
3 - AES
3
Input  AID tnumber (3 bytes hex): A10000

Input maximal key number: (1 - 14)3
 Choose application master key settings:
0 - No settings
1 - Settings not changeable anymore
2 - Create or delete file with master key authentication
3 - Master key not changeable anymore
4 - Settings not changeable anymore and create or delete file with master key
5 - Settings and master key not changeable anymore
6 - Create and delete file with master key and master key is not changeable anymore
7 - Settings not changeable anymore, create or delete file with master key, master key is not changeable anymore

2
=============
OK
Execution time of operation = 196 ms

Application created
-------------------------------------------------------
```

1.19. Delete application (h)

Enter AID to delete.

```
-----------------------------------------------
Input AID to delete (3 bytes hex): A10000
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 184 ms
-----------------------------------------------
```

1.20. Make file (j)

In configuration file set the AID and application master key.
For example make Standard Data File, size 100 bytes, enciphered communication.

```
-----------------------------------------------
Input File ID: 1
Choose communication mode:
 1 - PLAIN.
 2 - MACKED.
 3 - ENCIPHERED.
3
Choose file type:
 1 - Standard data file
 2 - Value file
 3 - Linear record file
 4 - Cyclic record file
1
Enter Read key number: 0
Enter Write key number: 0
Enter Read/Write key number: 0
Enter Change key number: 0
Enter size of the file you wish to create: 100
=============
OK
Execution time of operation = 90 ms


File created
-----------------------------------------------
```

Example: Make value file. Lower limit is 0, upper limit is 200, initial value is 100. Enciphered communication mode.

```
------------------------------------------------------
Input File ID: 2
Choose communication mode:
 1 - PLAIN.
 2 - MACKED.
 3 - ENCIPHERED.
3
Choose file type:
 1 - Standard data file
 2 - Value file
 3 - Linear record file
 4 - Cyclic record file
2
Enter Read key number: 0
Enter Write key number: 0
Enter Read/Write key number: 0
Enter Change key number: 0
Enter lower limit of your Value file: 0
Enter upper limit of your Value file: 200
Enter value of your Value file: 100
Do you wish to enable Limited credit?
 1 - Yes
 2 - No
2
Do you wish to enable Free get value?
 1 - Yes
 2 - No
2
=============
OK
Execution time of operation = 84 ms


File created
------------------------------------------------------
```

Example: Make linear record file. Size of record is 100, maximal number of records is 3, enciphered communication mode.

```
------------------------------------------------------
Input File ID: 3
Choose communication mode:
 1 - PLAIN.
 2 - MACKED.
 3 - ENCIPHERED.
3
Choose file type:
 1 - Standard data file
 2 - Value file
 3 - Linear record file
 4 - Cyclic record file
3
Enter Read key number: 0
Enter Write key number: 0
Enter Read/Write key number: 0
Enter Change key number: 0
Enter size of record: 100
Enter maximal number of records: 3
=============
OK
Execution time of operation = 100 ms


File created
------------------------------------------------------
```

1.21. Delete file (k)

In configuration file set the AID, and application master key. Enter File ID for deleting.

```
--------------------------------------------------
Enter file ID to delete:
1
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 83 ms
--------------------------------------------------
```

1.22. Write Std file or Record (l)

In configuration file set the AID, application key for Write or Read&Write access, and File ID.
For example write text to Standard data file, enciphered communication mode. Text read from file write.txt.
Size of text must be less or equal to size of file.

```
--------------------------------------------------
Choose file type:
 1 - Standard data file
 2 - Record file
1

Choose communication mode:
 1 - PLAIN.
 2 - MACKED.
 3 - ENCIPHERED.
3
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 82 ms
--------------------------------------------------
```

Example: Write record file.

```
--------------------------------------------------
Choose file type:
 1 - Standard data file
 2 - Record file
2

Choose communication mode:
 1 - PLAIN.
 2 - MACKED.
 3 - ENCIPHERED.
3
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 114 ms
--------------------------------------------------
```

1.23. Read Std file or Records (m)

In configuration file set the AID, application master key, and File ID.
For example read data from Standard data file, enciphered communication mode. Readed data will be saved into read.txt file.

Example: Read two records.

1.24. Read value file (n)

In the configuration file set authentication key, AID, AID key number for reading, and File ID.

1.25. Increase value file (o)

In the configuration file set authentication key, AID, AID key number for Read&Write access, and File ID.
Example: Increase value file by 20.

```
Choose communication mode:
 1 - PLAIN.
 2 - MACKED.
 3 - ENCIPHERED.
3

Value for increasing:
20
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 90 ms
Value increased by: 20
```

1.26. Decrease value file (p)

In the configuration file set authentication key, AID, AID key number for Read, Write or Read&Write access, and File ID.
Example: Decrease value file by 20.

```
Choose communication mode:
 1 - PLAIN.
 2 - MACKED.
 3 - ENCIPHERED.
3

Value for decreasing:
20
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 90 ms
Value decreased by: 20
```

1.27. Clear record file (q)

In the configuration file set authentication key, AID, AID key number for Read&Write access, and File ID. All records in the Linear or Cyclic Record file will be deleted.

```
Operation completed
Function status is: [0x00 (0)] UFR_OK
Card status is: CARD_OPERATION_OK
Execution time: 85 ms
All records deleted
```

1.28. Get Application AIDs (r)

In the configuration file set card master authentication key, AID = 0x000000.

```
-------------------------------------------------------------
Found 3 application IDs:
A10000
D10000
D30000
Execution time: 162 ms
-------------------------------------------------------------
```

1.29. Store key into SAM (s)

First select card key type, and enter value of key and ordinal key number into SAM from 1 to 127 (if user has access right for this key). Then enter host authentication key ordinal number, version of host authentication key, and value of AES authentication key.

For example enter 3K3DES key 0102030405060708090A0B0C0D0E0F101112131415161718 into SAM key number 125 with SAM host authentication with AES host key 11111111111111111111111111111111, key number 126 and key version 10.

```
-------------------------------------------------------------
SAM is opened
Enter key type
1 - DES (8 bytes)
2 - 2K3DES (16 bytes)
3 - 3K3DES (24 bytes)
4 - AES (16 bytes)
3
Input new 3K3DES key (24 bytes):
0102030405060708090A0B0C0D0E0F101112131415161718
Enter SAM ordinal key number (1 - 127):
125
Enter SAM key for host authentication ordinal number:
126
Enter version of host authentication key (0 - 255):
10
Enter host authentication key:
Enter AES key (16 bytes):
11111111111111111111111111111111
Host authentication is OK
Desfire key stored successfully
-------------------------------------------------------------
```

Revision history

Date	Version	Comment
2019-09-12	1.3	SAM keys support
2019-08-12	1.2	DES, 2K3DES and 3K3DES keys support